

Subject: NetScout Meeting
From: "Lundwall, Elizabeth" <Elizabeth.Lundwall@netscout.com>
Date: 10/23/2013 4:44 PM
To: "david.shive@gsa.gov" <david.shive@gsa.gov>

David,

I just left a message on your voice mail, but thought I would go ahead and send an email in case it is easier for you to respond to. I work for Scott Burgess, the local account manager for NetScout. He would very much appreciate the opportunity to meet with you to discuss our Network & Application performance monitoring/troubleshooting solution and discuss how it can help make your teams more proactive and allow for better collaboration across the IT organization. We can also help extend your investment in your existing tools and help reduce the need to purchase additional tools. I'm not sure how familiar you are with NetScout, but we added a lot of new capabilities this past year and in June we came out with a new release that totally changed how everything looks and feels. So if you've met with us before or think you know what NetScout is all about, it might be worth your time to take another look.

To give you a very general overview, our solution gives you a dashboard view into your environment and learns what's normal so we can proactively alert you to problems before your end-users are impacted. Not only are we able to give you a real-time view into your environment, we also give you the ability to rewind and go back in time to troubleshoot a problem. You can very quickly identify a problem in the dashboard and drill down to the flows and all the way to the packets if necessary in 3 clicks. A couple of new capabilities that I was most excited about are Auto Dependency Mapping and our new Packet Flow Switch that allows you to aggregate traffic or send a copy of the same traffic to multiple places. Please let me know if you might have any availability to meet on Nov. 5, 6 or 7. If those dates don't work for you, please let me know your first availability. I appreciate your consideration and look forward to your response.

Thank you,
Elizabeth Lundwall
NetScout Systems, Inc
972-713-4412 Direct
elizabeth.lundwall@netscout.com

Subject: Two Weeks Left: Register Today for a Free Expo Pass
From: "Interop Las Vegas" <interop@techwebliveevents.com>
Date: 3/18/2014 3:37 PM
To: david.shive@gsa.gov

View the [web version](#).

INTEROP Las Vegas

**CELEBRATING THE IT
COMMUNITY**

APRIL 4, 2014 / EXPO: APRIL 1-3 / MANDALAY BAY CONVENTION CENTER, LAS VEGAS

Two Weeks Left: Register Today for a Free Expo Pass*

A complimentary Expo Pass to [Interop Las Vegas](#) gives you the opportunity to see what's new, learn what's cutting edge and identify technology must-haves for your business. Evaluate products side-by-side and learn about innovations that will help you drive revenue and improve efficiencies.

**CLAIM YOUR FREE EXPO PASS
TODAY**

Free Expo Pass Extras at the IT Event of the Year

- Meet with over [350+ exhibitors](#) covering a wide range of products and solutions in the Expo Hall and take advantage of a host of other opportunities
- [Keynotes](#) from industry-leaders including:
 - Stephen Gillett, COO, Symantec
 - Rebecca Jacoby, CIO & Senior VP, Cisco
 - Larry Quinlan, Global CIO, Deloitte
- [Start-up Hot Seat](#) - Some of the most innovative new technologies come from startups, but doing business with them can be risky. In this high-energy session, we'll introduce five compelling startups in enterprise IT, and ask the hard questions you need answers to before engaging with them
- [Women in IT Panel & Luncheon](#) - Join your peers for an open forum to discuss how to advance in an IT organization, keep your skills sharp, build fruitful relationships with colleagues, learn effective dispute resolution techniques, and build a mentoring network
- Free InformationWeek sessions in the Interop HQ on the Expo Floor ([How to Be a Tech Blogger](#), [So You Want to Be a CIO?](#), [IT Change: Revolution or Evolution](#))
- [IDC Breakfast Briefing](#) - Join IDC's Rohit Mehra and a team of enterprise

communications and datacenter network analysts for a complimentary briefing and breakfast on Wednesday

- Complimentary [vendor tech sessions](#) presented by Aria Systems, Cisco, HP, Moovweb, NetIQ, NetScout, and more
- [InteropNet Classes and Tours](#) – See Interop's real-time network of the newest gear supporting the latest standards – all interoperating with each other. Classes and tours are available
- Interactive experiences on the Expo Floor including:
 - Tuesday Night Welcome Reception
 - Wednesday Booth Crawl
 - Passport Program
 - Interop Fun Zone
 - Interop Store
 - Best of Interop Awards Ceremony

[Register for a Free Expo Pass »](#)

Celebrating the IT Community

[f t in yt](#)

*Discount cannot be combined with other offers including group discounts or previously purchased passes. Discount ends Monday, March 28, 2014 11:59PM Pacific. Offer good on new registrations only. Prices after discount applied: Expo Only: Free.

Interop Las Vegas c/o UBM Tech
303 Second St., Suite 900 South Tower, San Francisco, CA 94107

UBM Tech

UNSUBSCRIBE from Interop Las Vegas

This email was sent to david.shive@gsa.gov. If this e-mail was forwarded to you and you would like to subscribe to our mailing list, please visit our [website](#). Add interop@techwebliveevents.com to your address book to ensure delivery to your inbox. Please do not reply to this message as responses are not monitored.

© UBM Tech 2014. All Rights Reserved. [Privacy Policy](#)

Subject: Continuous Forensic Analytics Buyer's Guide
From: NSS Labs <advisor@nsslabs.com>
Date: 6/17/2015 8:03 AM
To: david.shive@gsa.gov

 Research and Testing Banner

Continuous Forensic Analytics Buyer's Guide

Enterprises have long understood the need for technologies that provide detection of malicious activity. More recently, enterprises have become aware of the need for enhanced incident forensics, or rather for a layer of security that permits visibility into the clues left by covert digital activity.

NSS Labs defines continuous forensic analytics (CFA) as the process of performing full packet capture and session reconstruction and of mining and rapidly querying captured data. As an organization's primary investigation tool, a CFA system could also discover indicators of compromise (IOC), and it would have the ability to aggregate data from multiple sources (for example, logs, flow data, endpoints, and threat intelligence feeds).

Continuous forensic analytics bridges the gap that has existed between real-time visibility into threats and post-incident investigation of threats, and the CFA system is well positioned to become the über security console for organizations. Today's organizations understand the importance of tracking an invisible foe – and this is the value of continuous forensic analytics.

The following vendors are discussed in this edition of the Continuous Forensic Analytics Buyer's Guide:

Blue Coat	Fidelis Cybersecurity
IBM	NetScout
RSA	Niksun
WildPackets	Novetta

Read more in our [Continuous Forensic Analytics Buyer's Guide](#)

For more information about NSS Research & Testing, go to nsslabs.com.

Best Regards,

Subscriptions Starting at \$3,995

[Click here to learn more.](#)

Choose an NSS Subscription package that scales to fit your needs.

- **Professional**
- **Enterprise**
- **Enterprise Elite**
- **Investor**

Starting at \$3,995, a Professional subscription includes year-long access to the following test reports and analysis:

- **Test Reports** for all tested products
- **Comparative Reports** from the viewpoint of Security, Performance, and TCO
- **Security Value Map™** reports tie it all together providing a snapshot of findings

NSS Labs is the world's leading information security research and advisory company. With over 2 million man hours testing all of the leading security technologies, only NSS Labs truly understands which vendors and products live up to their marketing claims and which do not.

The Team at NSS Labs



NSS Labs, Inc. 206 Wild Basin Rd., Bldg A, Suite 200 Austin, TX 78746
[Contact Us](#) [Unsubscribe](#)

Subject: Morning Consult Tech: Week in Review & What's Ahead

From: "Morning Consult" <tech@morningconsult.com>

Date: 7/12/2015 5:00 PM

To: david.shive@gsa.gov



by [Amir Nasr](#) (@ameerkatmanor)

[Universities Increasingly Falling Victim to Cyberattacks](#)
from Morning Consult by Amir Nasr

If you're looking for information on pretty much any topic, a university is a good place to start. Hackers are now using the same logic, launching cyberattacks on institutions of higher education to access personal information on thousands of students, faculty and staff. Hundreds of data breaches over the past decade suggest that U.S. universities are a promising hunting ground for cyber thieves looking to obtain valuable identification information.

Week in Review

OPM Breach Aftermath Intensifies

The Director of the Office of Personnel Management, Katherine Archuleta, [resigned](#) a day after her office [revealed](#) that two data breaches compromised records for about 22 million people, reversing her early stance that she [would not](#) step down.

Another federal employee union, the National Treasury Employees Union, filed a class-action [lawsuit](#) against OPM and Archuleta.

A Morning Consult poll [showed](#) that many voters wanted to see some sort of punishment for Archuleta; 45 percent said she should be fired or suspended.

Car-riding Services, Here and Abroad

Uber continued its [fight](#) against a lawsuit in California that could decide whether its drivers are independent contractors or employees. Hundreds of Uber drivers provided statements defending the company.

Google-owned Waze [launched](#) its worldwide carpool pilot program in Israel.

Encryption Back in the Spotlight

Washington and Silicon Valley [remain divided](#) on whether back doors to encryption help law enforcement or harm consumers.

A paper authored by a group of prominent cryptographers, computer scientists and security specialists came to the [conclusion](#) that the U.S. and U.K. governments put some of the world's most

confidential information and critical infrastructure at risk by demanding special access to encrypted communications.

Encryption has also been targeted by FBI Director James Comey, who said the self-proclaimed Islamic State terrorist network uses encryption and Twitter to [recruit](#) English-speaking followers and send out kill orders.

What's Ahead

Senators are planning to [ask](#) for further information on how a glitch in software caused the New York Stock Exchange to shut down for more than three hours last week.

As the Federal Communications Commission continues to look into Charter's merger with Time Warner Cable and Bright House, some Democratic senators are calling on the FCC to [detail](#) the potential effects on consumers.

Mark Your Calendars (All Times Eastern)

Monday

No events scheduled.

Earnings Report: [Cloud Security Corp.](#)

Tuesday

House Energy and Commerce Committee holds a [hearing](#) on "Promoting Broadband Infrastructure Investment" @ 10 a.m.

Urban Institute holds a [discussion](#) on "Machine Learning in a Data-Driven World: What Does It Mean for Public Policy?" @ 10:30 a.m.

House Science, Space and Technology Committee holds second part of a [hearing](#) on "Advancing Commercial Weather Data: Collaborative Efforts to Improve Forecasts" @ 10 a.m.

Earnings Report: [Puget Technologies Inc.](#)

Wednesday

Access hosts its Crypto [Summit](#) on "key questions in the debate over encryption" @ 8 a.m.

Information Technology & Innovation Foundation hosts a [debate](#) titled

“Technology: Problem Solver or Dangerous Master?” @ 9 a.m.

House Small Business Committee holds a [hearing](#) on “Taking Flight: Small Business Utilization of Unmanned Aircraft” @ 11 a.m.

Hudson Institute [discusses](#) “Collaborative Governance and Security: A Stronger Internet for the Future” @ 12 p.m.

House Oversight and Government Reform Committee holds a [hearing](#) on cybersecurity @ 2 p.m.

Earnings Report: [Intel Corp.](#)

Thursday

Defense One holds [discussion](#) on “Big Data: Predicting The Next DOD Insider Threat” @ 8:30 a.m.

Politico hosts a [discussion](#) on “Outside, In: Aging in a Tech World” @ 11:45 a.m.

Earnings Report: [Google Inc.](#)

Friday

Advisory Committee to the Congressional Internet Caucus holds a [briefing](#) titled “Taylor Swift or Congress? Who Has More Power in the Digital Music Streaming Marketplace?” @ 12 p.m.

Earnings Report: [NetScout Systems Inc.](#)

Morning Consult Top Tech Reads

1) [Eric Holder: The Justice Department could strike deal with Edward Snowden](#)

from Yahoo News by Michael Isikoff

2) [Look at the damage Apple has done to Samsung — in one chart](#)

from Business Insider by Jim Edwards

3) [Farm Use of Drones to Take Off as Feds Loosen Restrictions](#)

from the Associated Press by Mary Clare Jalonick

4) [A Timeline of Government Data Breaches](#)

from National Journal by Kaveh Waddell and Stephanie Stamm



5) [Security Experts Oppose Government Access to Encrypted Communication](#)

from the New York Times by Nicole Perlroth

6) [These are the first 500 companies allowed to fly drones over the US](#)

from The Verge by Ben Popper

7) [Google's Waze to launch worldwide carpooling pilot in Israel](#)

from Haaretz by Amir Teig

8) [The Secret Startup That Saved the Worst Website in America](#)

from The Atlantic by Robinson Meyer

9) [We've finally hit the breaking point for the original Internet](#)

from the Washington Post by Brian Fung

10) [Gender, Political Divide on Public's Trust in Driverless Cars](#)
from Morning Consult by Tess Danielson



SUBSCRIBE



Subject: Morning Consult Tech: OPM Hack May Have 40-Year Impact; FTC Looking Into Apple's New Music Service
From: "Morning Consult" <tech@morningconsult.com>
Date: 7/13/2015 9:09 AM
To: David Shive <david.shive@gsa.gov>

by [Amir Nasr](#) (@ameerkatmanor)

Today's Washington Brief

- The data breaches at the Office of Personnel Management may not be fully realized for 40 years, when many of those who had information stolen have retired. ([FedScoop](#))
- Lawmakers on Capitol Hill may strip OPM of its control over security clearances following two data breaches that compromised records for about 22 million people. ([The Hill](#))
- A government entity may be behind the massive cyberattack that penetrated the Italian cybersecurity firm Hacking Team. ([Reuters](#))

Today's Business Brief

- The Federal Trade Commission is looking into claims that Apple's new music streaming service and its treatment of rival companies may violate antitrust laws. ([Reuters](#))
- Public interest groups say the decision from the Supreme Court to not hear a copyright case between Google and Oracle could have serious implications for the future of software development. ([The Hill](#))
- Patrick Liu, president of the digital entertainment unit at Alibaba Group Holding Ltd., will receive legal support from his company after being taken into policy custody. ([Bloomberg](#))

Today's Chart Review

[Patent troll lawsuits head toward all-time high](#) from Ars Technica

Mark Your Calendars (All Times Eastern)

Monday

No events scheduled.

Earnings Report: [Cloud Security Corp.](#)

Tuesday

House Energy and Commerce Committee holds a [hearing](#) on “Promoting Broadband Infrastructure Investment” @ 10 a.m.

Urban Institute holds a [discussion](#) on “Machine Learning in a Data-Driven World: What Does It Mean for Public Policy?” @ 10:30 a.m.

House Science, Space and Technology Committee holds second part of a [hearing](#) on “Advancing Commercial Weather Data: Collaborative Efforts to Improve Forecasts” @ 10 a.m.

A bipartisan group of senators and representatives hold a [press conference](#) to oppose the Innovation Act @ 2 p.m.

Earnings Report: [Puget Technologies Inc.](#)

Wednesday

Access hosts its Crypto [Summit](#) on “key questions in the debate over encryption” @ 8 a.m.

Information Technology & Innovation Foundation hosts a [debate](#) titled “Technology: Problem Solver or Dangerous Master?” @ 9 a.m.

House Small Business Committee holds a [hearing](#) on “Taking Flight: Small Business Utilization of Unmanned Aircraft” @ 11 a.m.

Hudson Institute [discusses](#) “Collaborative Governance and Security: A Stronger Internet for the Future” @ 12 p.m.

House Oversight and Government Reform Committee holds a [hearing](#) on cybersecurity @ 2 p.m.

Earnings Report: [Intel Corp.](#)

Thursday

Defense One holds [discussion](#) on “Big Data: Predicting The Next DOD Insider Threat” @ 8:30 a.m.

Politico hosts a [discussion](#) on “Outside, In: Aging in a Tech World” @ 11:45 a.m.

Earnings Report: [Google Inc.](#)

Friday

Advisory Committee to the Congressional Internet Caucus holds a [briefing](#) titled “Taylor Swift or Congress? Who Has More Power in the Digital Music Streaming Marketplace?” @ 12 p.m.

TechFreedom hosts [event](#) on “restoring Internet independence,” featuring remarks from FCC Commissioner Ajit Pai @ 8 p.m.

Earnings Report: [NetScout Systems Inc.](#)

General

**[FTC exploring Apple rules for streaming music rivals in App Store](#)
from Reuters by Diane Bartz and Julia Love**

U.S. government antitrust regulators are looking into claims about whether Apple’s treatment of rival streaming music apps is illegal under antitrust law.

**[Spotify makes case against Apple in Congress](#)
from Politico by Tony Romm**

Spotify’s lobbyists have quietly made the rounds in D.C., whispering to lawmakers for months that Apple’s new music offering threatens to stifle its competitors. The apparent goal has been to raise antitrust suspicions about the iPhone giant, which faced a previous government lawsuit over its pricing of e-books.

**[Alibaba to Give Legal Support as Unit’s President Held by Police](#)
from Bloomberg News by Lulu Yilun Chen**

Alibaba Group Holding Ltd. will provide legal support to Patrick Liu, president of its digital entertainment unit, after he was taken into police

custody.

Ellen Pao Is Out as CEO of Reddit
from the Wall Street Journal by Jeff Elder

Reddit, one of the most highly trafficked websites in the world, is replacing its interim chief executive, Ellen Pao, ending an eight-month tenure that was enmeshed in controversy.

How Washington is getting ready for the fiber-optic future of communications
from the Washington Post by Brian Fung

In moving us onto ever newer, ever faster networks, America's telecom firms are phasing out their old copper lines and installing high-speed fiber optics. The result? Soon, all our phone calls will be handled by the nation's carriers as data packets.

AT&T can punish employees for wearing 'prisoner' T-shirts to work, a court rules
from the Washington Post by Brian Fung

AT&T didn't break the law when it forbade its technicians and other public-facing employees from wearing T-shirts emblazoned with the words "Inmate" and "Prisoner of AT&T," a federal appeals court ruled.

Silicon Valley Company Starts to Take Court Disputes Online
from the Associated Press by Sudin Thanawala

A Silicon Valley company is starting to make software that experts say represents the next wave of technology in which the law is turned into computer code that can solve legal battles without the need for a judge or attorney.

Arizona makes deal with ACLU, won't enforce bad law on "revenge porn"
from Ars Technica by Joe Mullin

A lawsuit filed in September by the American Civil Liberties Union, along with a group of booksellers and publishers, has put a stop to Arizona's "revenge porn" law.

Outspoken privacy campaigner Caspar Bowden dies after battle with cancer

from The Guardian by Samuel Gibbs

Microsoft's former head of privacy and respected independent privacy campaigner Caspar Bowden has died after a battle with cancer. A popular and outspoken figure in privacy advocacy, Bowden was particularly active after the Snowden revelations of government surveillance, advising the European parliament among others.

U.S. Index Futures Rise After Greece Reaches Deal With Creditors

from Bloomberg News by Inyoung Hwang

U.S. stock-index futures advanced, signaling equities will rally for a third day, after Greece reached an agreement with its creditors. Standard & Poor's 500 Index E-mini contracts expiring in September added 0.6 percent to 2,082.25 at 7:26 a.m.in New York. Contracts on the Dow Jones Industrial Average climbed 114 points, or 0.7 percent, to 17,783.

Immigration

Boehner blames Obama for immigration inaction

from The Hill by Mike Lillis

Rep. John Boehner (R-Ohio) is putting the blame for Congress's failure to move immigration reform squarely on the shoulders of President Obama. The House Speaker said he's been pushing immigration reform since he took the gavel four years ago, but the president has "poisoned the well" with his executive actions on the issue.

Net Neutrality

Warren, Sanders want FCC to investigate high Internet prices

from The Hill by David McCabe

A group of Democratic senators are asking the Federal Communications Commission to look into pricing for Internet service around the country.

FCC Proposes Telecom Service Safeguards Amid Move to Fiber

from the Wall Street Journal by Ryan Knutson

U.S. regulators proposed new rules to make sure carriers such as AT&T Inc. and Verizon Communications Inc. keep offering the same level of service as they replace their aging copper networks with fiber.

Intellectual Property

SCOTUS move fuels uncertainty for tech, groups say
from The Hill by David McCabe

The Supreme Court's decision to not weigh in on a copyright fight between Google and Oracle could have severe implications for future software development.

Patent troll lawsuits head toward all-time high
from Ars Technica by Joe Mullin

New patent statistics show that patent litigation, driven by so-called "patent trolls," could reach an all-time high in 2015. It's a statistic that's sure to be highlighted by tech lobbyists and others pushing for patent reform, given that the House is likely to take up a floor vote of the Innovation Act this month.

Telecommunications

Analysts: T-Mobile's strong Q2 subscriber numbers likely to boost revenue, crimp earnings and margins
from FierceWireless by Phil Goldstein

T-Mobile US' pre-release of its second-quarter subscriber numbers—which showed strong momentum, especially in postpaid subscribers—prompted financial analysts to raise their expectations for the carrier's revenue in the period. However, analysts also think T-Mobile's EBITDA and margins could come under pressure as a result.

Mobile & Social

Airbnb brings sharing economy under the microscope
from CNET by Dara Kerr

The home-sharing site learns the hard way that it can't assume San

Francisco supervisors won't change their minds — even after they passed a law legalizing short-term rentals.

Data

Privacy advocates ask regulators to take a closer look at gadgets that are 'always on'

from the Washington Post by Hayley Tsukayama

The Electronic Privacy Information Center (EPIC) would like regulators to delve deeper into the privacy implications of devices, such as those with voice-controls that are “always on.” The group posted a letter to the Federal Trade Commission and the Justice Department asking for an investigation always-on technologies present in devices from Microsoft, Google, Amazon and others.

New proposal would strike at web's anonymity

from The Hill by Mario Trujillo

Privacy advocates, public interest groups and even some celebrities are raising alarms about a proposal that could limit the ability of some website owners to disguise themselves.

Cybersecurity

Impact of OPM breach could last more than 40 years

from FedScoop by Dan Verton

Intelligence and security experts say recovering from the massive data breach at the Office of Personnel Management won't happen until most retire.

Lawmakers look to strip OPM powers after hack

from The Hill by Cory Bennett

Lawmakers are debating whether to strip the Office of Personnel Management (OPM) of its control over security clearances after hackers made off with nearly 20 million background check forms housed at the agency.

Years of Tech Mismanagement Led to OPM Breach, Resignation of Chief

from the Wall Street Journal by Steven Norton and Clint Boulton

The massive cyberattacks that led to the resignation of Katherine Archuleta as head of the U.S. Office of Personnel Management followed years of audits that identified deficient systems and processes for managing technology.

New bill would protect OPM hack victims for life

from FedScoop by Greg Otto

The bill, drafted by senators from Maryland and Virginia, extends the protections offered by OPM in the wake of two data breaches.

Italian cyber-security firm suspects foreign government was behind mass attack

from Reuters by Crispian Balmer

Italian cyber-security firm Hacking Team said a government might have been behind a massive hack of its systems and warned that the subsequent leaking of its computer codes could prove a field day for criminals.

At White House, 30-day sprint kicks off cyber marathon to stop intrusions

from Reuters by Roberta Rampton

The federal government could find more cyber intrusions as it takes a close look at its sprawling and sometimes creaky systems in the wake of massive hacks.

What it took for Ethiopia to lose access to hacking tools it used against journalists in the U.S.

from the Washington Post by Andrea Peterson

Italian company Hacking Team, which was itself hacked, is part of a burgeoning commercial surveillance industry that critics allege sells hacking tools once reserved for the most advanced intelligence agencies to any country that can pay.

Hacked in the U.S.A.: China's Not-So-Hidden Infiltration Op
from Bloomberg News by Chris Strohm et al

U.S. authorities missed clues connecting one incident of cyberattack to the next. Interviews with federal investigators and cybersecurity experts paint a troubling portrait of what many are calling a serious failure of U.S. intelligence agencies to spot the pattern or warn potential victims. Moreover, the problems in Washington add new urgency to calls for vigilance in the private sector.

E-Commerce

Can mobile apps emerge sole driver of India's e-commerce?
from the Economic Times by Aparajita Gupta and Sharon Thambala

With 975 million mobile phone connections in India and penetration at 140 percent in urban areas, many e-commerce firms see apps as the way forward to push sales, with some even planning to make it their exclusive delivery platform. Is it feasible?

Opinions, Editorials & Perspectives

Computer glitches struck the stock market and United Airlines on the same day. Here's why you didn't believe it was a coincidence.
from the Washington Post by David J. Helfand

Early Wednesday morning, a computer network problem forced United Airlines to ground all of its planes. A couple of hours after they started flying again, the New York Stock Exchange halted trading for the same reason. It couldn't have been a coincidence!

Portents of World Cyberwar
from the Wall Street Journal by L. Gordon Crovitz

A new novel, "Ghost Fleet," warns Americans about advances in cyberwarfare that could leave the U.S. as unprepared as Britain was against the U-boats. The premise is that leapfrogging technologies can disrupt the Pentagon, as they have many civilian industries, and that new strategic thinking is difficult to achieve in a vast bureaucracy.

OPM got hacked and all I got was this stupid e-mail
from Ars Technica by Jonathon M. Gitlin

This data isn't mere credit card numbers that can be altered and reissued with minimal pain. It's our lives—histories, relationships, personal appearance, drug use, educational background, and much more—even biometrics. They can't be altered and reissued, and a few months of credit monitoring will do little to protect victims from those determined enough to pull off the heist in the first place.

Research Reports, Issue Briefs & Case Studies

The Future Of Data Security And Privacy: Growth And Competitive Differentiation
from Forrester by John Kindervag

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

SUBSCRIBE

*The Morning Consult
Morning Consult, P.O. Box 27068
Washington District of Columbia 20038
United States*

This email is intended for david.shive@gsa.gov.
[Update your preferences](#) or [Unsubscribe](#)

Subject: Morning Consult Tech: 2016 Shaping Up To Be An Uber Election; Google Capital Leads \$100 Million Investment in CrowdStrike
From: "Morning Consult" <tech@morningconsult.com>
Date: 7/14/2015 9:03 AM
To: David Shive <david.shive@gsa.gov>

by [Amir Nasr](#) (@ameerkatmanor)

Today's Washington Brief

- As the 2016 presidential race picks up steam, ride-sharing app Uber is shaping up to play a central role. ([Fusion](#))
- The Justice Department said it's aiming to build an "office of the future" through major technological upgrades for employee use. ([NextGov](#))
- Defense Secretary Ash Carter has plans for a high-tech military in the future. But new approaches might be needed in attempts to draw improved interest from millennials. ([FedScoop](#))

Today's Business Brief

- Google Capital led a \$100 million round of investment in CrowdStrike, an Irvine, Calif.-based firm whose head of investigations, Shawn Henry, comes from the Federal Bureau of Investigation's computer crimes division and has strong ties to Washington. ([Wall Street Journal](#))
- The Justice Department has been asked by groups acting as representation for thousands of authors, agents and independent booksellers to probe Amazon over possible violations of antitrust laws. ([New York Times](#))
- Google is looking to bring improved internet access to Cuba. ([Politico](#))

Today's Chart Review

[This chart shows why Wall Street is so worried about Google's business](#)

from Business Insider

Mark Your Calendars (All Times Eastern)

Tuesday

House Science, Space and Technology Committee holds second part of a [hearing](#) on “Advancing Commercial Weather Data: Collaborative Efforts to Improve Forecasts” @ 10 a.m.

Urban Institute holds a [discussion](#) on “Machine Learning in a Data-Driven World: What Does It Mean for Public Policy?” @ 10:30 a.m.

Earnings Report: [Puget Technologies Inc.](#)

Wednesday

Access hosts its Crypto [Summit](#) on “key questions in the debate over encryption” @ 8 a.m.

Information Technology & Innovation Foundation hosts a [debate](#) titled “Technology: Problem Solver or Dangerous Master?” @ 9 a.m.

House Small Business Committee holds a [hearing](#) on “Taking Flight: Small Business Utilization of Unmanned Aircraft” @ 11 a.m.

Hudson Institute [discusses](#) “Collaborative Governance and Security: A Stronger Internet for the Future” @ 12 p.m.

House Oversight and Government Reform Committee holds a [hearing](#) on cybersecurity @ 2 p.m.

Earnings Report: [Intel Corp.](#)

Thursday

Politico hosts a [discussion](#) on “Outside, In: Aging in a Tech World” @ 11:45 a.m.

Earnings Report: [Google Inc.](#)

Friday

Advisory Committee to the Congressional Internet Caucus holds a [briefing](#) titled “Taylor Swift or Congress? Who Has More Power in the Digital Music Streaming Marketplace?” @ 12 p.m.

TechFreedom hosts [event](#) on “restoring Internet independence,” featuring remarks from FCC Commissioner Ajit Pai @ 8 p.m.

Earnings Report: [NetScout Systems Inc.](#)

General

[Justice Department Plans Major Office Tech Upgrade](#) from NextGov by Hollie Golden

Citing evolving technology and an increasingly mobile workforce, the Department of Justice envisions an “office of the future,” which would upgrade much of the technology agency employees use.

[Google testing the waters in Cuba](#) from Politico by Nancy Scola

A Google executive is headed to Cuba this weekend to explore bringing better Internet access to the island, and the search giant has made a related proposal to the Cuban government.

[After drone diverts fire-fighting planes, lawmakers want fines and jail time](#) from Ars Technica by Megan Geuss

In late June, the Lake Fire burned through 30,000 acres of California wilderness in San Bernardino county. In order to keep the flames from encroaching on an area of nearby houses, the US Forest Service sent three planes filled with fire retardant to dump on an area of the fire. That cargo never reached its intended target, because the low-flying planes had to turn back when they encountered a drone... Now, lawmakers are introducing legislation to make sure it doesn't happen again.

[State-Owned Chinese Chip Maker Tsinghua Unigroup Makes \\$23 Billion Bid for Micron](#) from the Wall Street Journal by Eva Dou

China's Tsinghua Unigroup Ltd. has submitted a bid to buy out U.S. memory chip maker Micron Technology Inc. for \$23 billion.

2 visions emerge for getting self-driving cars on road **from the Associated Press by Dee-Ann Durbin**

Traditional automakers like Mercedes and Toyota already make vehicles equipped with systems that keep cars within their lanes, apply the brakes or park by themselves. Their plan is to gradually automate more functions of driving until, perhaps by 2025. But Google, Alibaba, Baidu and other tech companies are aggressively working on their own self-driving vehicles, and could leapfrog the car industry in bringing them to market. Google, for instance, promises to deliver a self-driving car in five years.

US Presidential Candidates' Internet Policies, Ranked **from Gizmodo by Adam Clark Estes**

With 20-odd US presidential candidates in the mix, everyone's trying to pick the winning position on the issues that matter most to Americans. The future of the internet is obviously a big one. Here's what's been proposed so far — the good, the bad, and the utterly insane.

U.S. Stock-Index Futures Little Changed Before Retail Sales Data **from Bloomberg News by Sofia Horta E Costa**

U.S. stock-index futures were little changed, after equities capped their biggest three-day rally of 2015, amid corporate earnings and as investors awaited data on retail sales. JPMorgan Chase & Co. advanced after its quarterly profit beat analysts' estimates as expenses fell. Johnson & Johnson added 0.7 percent after its earnings exceeded analysts forecasts and the company raised its full-year profit view. Wells Fargo & Co. slipped 0.8 percent after quarterly revenue missed estimates.

Immigration

Report: 1,800 Immigrants Re-Arrested After Release From Jail **from the Associated Press by Amy Taxin**

More than 1,800 immigrants that the federal government wanted to deport were nevertheless released from local jails and later re-arrested for various crimes.

Net Neutrality

COMPTEL, Sprint, XO, others urge FCC to “competify” the broadband industry

from FierceTelecom by Sean Buckley

A group of industry trade organizations and service providers have launched the “Competify” campaign to encourage the FCC to drive further competition in the broadband market.

Intellectual Property

Appeals court: Newegg can’t get fees from notorious patent troll

from Ars Technica by Joe Mullin

Online retailer Newegg has developed a reputation for fighting hard against the kind of non-practicing patent holders often called “patent trolls.” Now a long fight against one such entity, called SFA Systems, has reached a conclusion, and the US Court of Appeals for the Federal Circuit denied (PDF) Newegg’s request to have its legal fees paid.

Telecommunications

How consumers can fight back against big wireless

from CNET by Marguerite Reardon

A startup could allow wireless customers who are prohibited from filing class-action lawsuits to hold big companies like AT&T accountable when they violate their contracts.

Is this the end of the phone subsidy?

from the Washington Post by Hayley Tsukayama

For years, smartphone shopping has gone something like this: Pick the latest phone, pay a one-time fee of \$200 for it, and agree to a monthly rate for calls, texts and data... But AT&T has recently made a series of small changes, in their place are plans that eliminate the price break off the price tag of the phone — and spread that cost over 12, 18 or 24 months.

Mobile & Social

Welcome to the Uber election

from Fusion by Kevin Roose

Uber, a tech startup that was a provincial runt during the 2012 campaign, is poised to play a central role in 2016.

Republicans hail Uber in bid for tech cred

from Politico by Tony Romm

Republican White House hopefuls looking to boost their tech cred are racing to hitch a ride on Uber — while Democratic front-runner Hillary Clinton is keeping a cautious distance.

An Uber I.P.O. Looms, and Suddenly Bankers Are Using Uber. Coincidence?

from the New York Times by Nathaniel Popper

JPMorgan Chase announced that it would reimburse all of its employees for rides taken with Uber — offering access to “Uber’s expanding presence and seamless experience,” the company said in a news release.

One Company’s Plan to Turn Internet Flame Wars Into Campaign Gold

from National Journal by Zach Montellaro

Brigade wants to become the destination for user-driven political discussions on the Web—and gather a gold mine of information in the process.

Data

A \$200 privacy device has been killed, and no one knows why

from Ars Technica by Dan Goodin

A security researcher has abruptly cancelled next month’s scheduled unveiling of a privacy device designed to mask Internet users’ physical locations. It’s a move that has both disappointed privacy advocates and aroused suspicions.

Cybersecurity

Google Capital Leads \$100 Million Cybersecurity Investment

from the Wall Street Journal by Danny Yadron

Google Capital led a \$100 million investment in CrowdStrike, an Irvine, Calif., firm with deep ties to Washington. Its head of investigations, Shawn Henry, is the former top computer-crimes official at the Federal Bureau of Investigation. CrowdStrike's D.C.-based chief technology officer, Dmitri Alperovitch, has a long history of calling out foreign hacker groups.

Pentagon's 'force of the future' and America's disconnected millennials

from FedScoop by Dan Verton

Secretary of Defense Ash Carter's plans to build a future high-tech military may require new approaches to workforce development that are drastically different from that of previous generations.

OPM Hack: The Complete Timeline

from FedScoop by Grayson Ullman

FedScoop traces data compromises at OPM from the August 2014 hack through Director Katherine Archuleta's resignation.

It's not just OPM: Cybersecurity across the federal government is pretty awful

from the Washington Post by Andrea Peterson

The nation is still reeling from the revelation that hacks at the Office of Personnel Management exposed the personal data of 22.1 million people. But government audits reveal that the agency isn't alone: Basically the whole government is struggling to protect its computer systems.

After Monumental Breach, Banks and Even Farmers Are Buying NSA-Fueled Surveillance Gear

from NextGov by Aliya Sternstein

Agriculture companies are now buying cyber-surveillance gear fueled by National Security Agency intelligence. It is the same apparatus that discovered the monumental hack now known to have netted personal information on 21.5 million background check applicants and family members.

Hacking Team boss: we sold to Ethiopia but 'we're the good guys'
from The Guardian by Samuel Gibbs

David Vincenzetti, 47, founder of cybersecurity firm Hacking Team, told Italian newspaper La Stampa that the cyber attack – which saw the code for companies hacking tools and its email archive published online – was not enabled by poor security or weak passwords and that it could have only been an organisation “at the governmental level”.

Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments
from Vice Motherboard by Joshua Kopstein

The massive breach that leaked internal documents belonging to Hacking Team, the Italian spyware vendor, has already confirmed that the company sold its surveillance tech to some of the most brutal regimes around the world, along with some closer to home. Emails and documents from the 400 gigabyte mega-leak reveal a sprawling network of resellers—some of them based in the United States—that helped Hacking Team get its spy tech into the hands of a long list of government clients.

Hacking Team data breach provides links to Florida law enforcement
from the Tampa Bay Times by Trevor Aaronson

An Italian company that sells surveillance software to governments and law enforcement agencies worldwide is negotiating to provide a Florida police agency with spyware technology that infiltrates phones and computers.

N.J. State Police shopped for spy software, emails show
from Politico by Ryan Hutchins and Conor Skelding

The New Jersey State Police considered buying controversial spy software that can be used to remotely control smart phones and computers, even meeting in West Trenton with representatives of an Italian surveillance company now accused of selling the same technology to repressive governments around the world.

Why webcam indicator lights are lousy privacy safeguards
from the Christian Science Monitor by Malena Carollo

A recent academic study found that few computer users notice indicator lights and even fewer realize that the camera is always recording when the light is on. The lack of awareness, say researchers, makes people more vulnerable to webcam spying.

[This teen won't go to prison, even after he hacked 50,700 computers](#)

from the Washington Post by Jacob Bogage

Julius Kivimaki was 15 years old when he began a cybercrime spree that accessed 50,700 devices. And earlier this month, Kivimaki, now 17, was found guilty of many instances of “aggravated computer break-ins.” But the teenager won’t go to prison, or even face a hefty fine. He was sentenced to two years of suspended jail time, ordered to return the 6,588 euros, or \$7,000, he made via the hacks and had his personal computer confiscated.

[WikiLeaks Is Now a Target In the Massive Spam Attack on Bitcoin](#) **from Vice Motherboard by Jordan Pearson**

The Bitcoin network is being hammered by a massive spam attack, and the targets now include WikiLeaks and Voat, the upstart Reddit clone that became a home for Redditors fleeing the site after new anti-harassment policies were instituted.

E-Commerce

[Accusing Amazon of Antitrust Violations, Authors and Booksellers Demand Inquiry](#)

from the New York Times by David Streitfeld

Five years after Amazon secretly asked regulators to investigate leading publishers — a case that ended up reinforcing the e-commerce company’s clout — groups representing thousands of authors, agents and independent booksellers are asking the United States Department of Justice to examine Amazon for antitrust violations.

Opinions, Editorials & Perspectives

[Federal Cybersecurity Needs Improvement](#)

from Politico by Jeh Johnson

Our federal cybersecurity is not where it needs to be. In the case of the breach of the Office of Personnel Management, a large amount of highly personal and sensitive information was taken by a very sophisticated actor. In response, on June 12, the White House announced the establishment of a Cybersecurity Sprint Team, to conduct a 30-day review of the federal government's cybersecurity policies and practices. This response is part of a much broader federal cybersecurity effort that has been underway for some time.

Timing is everything for securing wireless communications

from the Christian Science Monitor by Steven Chabinski

Even though disrupting wireless communications – whether cellphone networks or GPS – could harm the US economy and put lives at risk, these networks remain far too vulnerable to attacks.

FCC's Lifeline Program Ripe for Fraud, Abuse

from Politico by Mike O'Rielly and Rep. Marsha Blackburn

The Federal Communications Commission's low-income program, known formally as Lifeline, has spent billions of ratepayer dollars to provide phone service for poorer Americans. Because of significant waste, fraud and abuse in the program, however, a good portion of that funding has not been used as intended.

Java Was Really Insecure For a While. Then It Got Better. Now There's a New Problem.

from Slate by Lily Hay Newman

Java is a popular programming language often used on websites to deliver multimedia content. After frequent attacks and cybersecurity problems in versions 6 and 7, owner Oracle released Java 8 to help remedy the situation. It's been almost two years since Java has had a zero-day vulnerability (an exploit with no patch), but the party is over.

America's secret weapon against cyber attacks? Try a new military for cyber crimes

from Fortune by Andrew Rubin

It is time for the nation to create a sixth branch of the military dedicated to cyber security with its own service academy.

Overlooking innovation: The need to include Silicon Valley in the military-industrial complex

from the Brookings Institution by Brendan Orino

Through a series of interviews with Silicon Valley venture capitalists and executives, traditional defense industrial base representatives, and government officials, Federal Executive Fellow Jason Tama puts his finger on one of the perennial hot-button questions in Washington: Why can't the Pentagon (and federal government overall) attract new, innovative entrants to the military-industrial complex?

Research Reports, Issue Briefs & Case Studies

Key findings from the 2015 US State of Cybercrime Survey
from PricewaterhouseCoopers

Cybersecurity incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors. This report found rising concern among the 500 US executives, security experts, and others from the public and private sectors who participated

The Future of Voting: End-to-End Verifiable Internet Voting – Specification and Feasibility Study
from the U.S. Vote Foundation

This report examines the future of voting and the possibility of conducting secure elections online. Specifically, it explores whether End-to-End Verifiable Internet Voting (E2E-VIV) systems are a viable and responsible alternative to traditional election systems.

SUBSCRIBE

*The Morning Consult
Morning Consult, P.O. Box 27068
Washington District of Columbia 20038
United States*

This email is intended for david.shive@gsa.gov.
[Update your preferences](#) or [Unsubscribe](#)

Subject: Morning Consult Tech: Iran's Tech Sector to Benefit From Nuclear Deal; Tsinghua's Bid for Micron Expected to Draw Regulatory Scrutiny
From: "Morning Consult" <tech@morningconsult.com>
Date: 7/15/2015 8:39 AM
To: David Shive <david.shive@gsa.gov>

by [Amir Nasr](#) (@ameerkatmanor)

Today's Washington Brief

- The recent deal struck between the United States, European powers and Iran is extremely promising for Iran's tech industry. ([Washington Post](#))
- None of the 21.5 million Americans who had personal information exposed in the Office of Personnel Management data breaches have received official notification from a government agency. ([Reuters](#))
- The USA Freedom Act permits the National Security Agency to temporarily continue its bulk data collection in the United States. The American Civil Liberties Union has asked an appellate court to stop the practice. ([Ars Technica](#))

Today's Business Brief

- Micron Technology Inc. has seen its shares rise in light of a recent bid from Chinese company Tsinghua Unigroup Ltd., despite expected scrutiny from federal regulators. ([Wall Street Journal](#))
- A fake news article claiming an offer had been made to takeover Twitter led to a sudden spike in the company's shares. The U.S. Securities and Exchange Commission is looking into the matter. ([Bloomberg News](#))
- A new campaign, Competify, aims to push back against consolidation in the broadband market. The PR push comes as the Federal Communications Commission reviews Charter Communication's proposed takeover of Time Warner Cable Inc. and Bright House Networks LLC. ([Morning Consult](#))

Today's Chart Review

[Twitter Stock Spikes on Fake Bloomberg Report](#)
from Slate

Mark Your Calendars (All Times Eastern)

Wednesday

Access hosts its Crypto [Summit](#) on “key questions in the debate over encryption” @ 8 a.m.

Information Technology & Innovation Foundation hosts a [debate](#) titled “Technology: Problem Solver or Dangerous Master?” @ 9 a.m.

House Small Business Committee holds a [hearing](#) on “Taking Flight: Small Business Utilization of Unmanned Aircraft” @ 11 a.m.

Hudson Institute [discusses](#) “Collaborative Governance and Security: A Stronger Internet for the Future” @ 12 p.m.

House Oversight and Government Reform Committee holds a [hearing](#) on cybersecurity @ 2 p.m.

Earnings Report: [Intel Corp.](#)

Thursday

Politico hosts a [discussion](#) on “Outside, In: Aging in a Tech World” @ 11:45 a.m.

Earnings Report: [Google Inc.](#)

Friday

Advisory Committee to the Congressional Internet Caucus holds a [briefing](#) titled “Taylor Swift or Congress? Who Has More Power in the Digital Music Streaming Marketplace?” @ 12 p.m.

TechFreedom hosts [event](#) on “restoring Internet independence,” featuring remarks from FCC Commissioner Ajit Pai @ 8 p.m.

Earnings Report: [NetScout Systems Inc.](#)

General

What the Iran deal means for the country's surprisingly strong tech industry

from the Washington Post by Brian Fung

The deal to scale back Iran's uranium enrichment program still has to be approved by Congress and Iranian officials. But if it moves ahead, analysts say, there's at least one group that'll unquestionably benefit from the move, and that's Iran's burgeoning tech sector.

Micron Shares Jump on Tsinghua Bid Despite Expected U.S. Regulatory Scrutiny

from the Wall Street Journal by Liz Hoffman and William Mauldin

A bid from China's Tsinghua Unigroup Ltd. to buy Micron Technology Inc. was greeted warmly by the U.S. chip maker's shareholders Tuesday. It is far from certain, though, that the audacious move will succeed given expected resistance from Micron and U.S. regulators.

San Francisco tightens 'Airbnb law' with new amendment

from CNET by Dara Kerr

San Francisco's board of supervisors passed an amendment tightening the rules governing short-term room and home rentals in the city. This means people offering accommodations through Airbnb — a popular room- and home-sharing platform — may face closer scrutiny.

Self-driving Cars May End the Fines That Fill City Coffers

from Wired by Alex Davies

Once there are self-driving cars, it's a safe bet we won't do things like speed, run reds, park illegally, or drive drunk. And that means we won't be fined for doing those things. That's going to put the squeeze on city budgets, according to a Brookings Institution report.

White House: We Need More Tech to Handle an Aging America

from Wired by Issie Lapowsky

This week, the White House is kicking off its Conference on Aging, the once-a-decade gathering that has given birth to landmark government

programs like Medicare and Medicaid.

Laura Poitras Sues U.S. Government to Find Out Why She Was Repeatedly Stopped at the Border
from The Intercept by Jenna McLaughlin

Over six years, filmmaker Laura Poitras was searched, interrogated and detained more than 50 times at U.S. and foreign airports. When she asked why, U.S. agencies wouldn't say.

U.S. Stock-Index Futures Little Changed Before Yellen Testimony
from Bloomberg News by Alan Soughley and Roxana Zega

Standard & Poor's 500 Index E-mini contracts expiring in September added 0.1 percent to 2,103.75 at 7:29 a.m. in New York. Contracts on the Dow Jones Industrial Average climbed 13 points, or 0.1 percent, to 17,974.

Immigration

Martin O'Malley Pledges to Go Further Than Obama on Immigration
from Time by Sam Frizell

Former Maryland Gov. Martin O'Malley called for a broad sweep of executive actions to protect undocumented immigrants from deportation and detention, touting his work as governor of Maryland and saying he would go further than President Obama as he seeks to attract the support of Hispanic voters.

Net Neutrality

Here's how data caps really affect your Internet use, according to data
from the Washington Post by Brian Fung

It turns out that data caps are incredibly effective at getting people to use less data, and not merely on cellphone plans. A new paper published by the National Bureau of Economic Research takes actual, real-world data on data usage from a North American Internet provider and shows that even for people on fixed, wired home broadband, data caps have a dramatic effect on consumer behavior.

Intellectual Property

CBO: Budget effect of House patent bill insignificant **from The Hill by Mario Trujillo**

A House bill to rein in abusive litigation tactics of so-called patent trolls will have an insignificant effect on the government's budget, according to the Congressional Budget Office.

Apple Is Getting Sued Over the Name iWatch, Even Though That's Not What Its Product Is Called **from Bloomberg News by Daniele Lepido**

Type "iWatch" into Google's search engine, and the top result is likely to be an ad for the Apple Watch. Apple pays Google for the advertisements so it doesn't miss out on potential customers who entered the wrong product name. But Probandi, a small Dublin-based company, which owns the iWatch trademark in Europe, is hoping the ads will cost Apple a lot more.

Telecommunications

Tech Coalition Decries Effects of Telecom Consolidation on Competition **from Morning Consult by Amir Nasr**

Competify, a campaign launched on Monday, says they're aiming to cure the "chronic disease caused by a few huge companies that control access to America's critical broadband infrastructure." The PR push comes as the Federal Communications Commission reviews the proposed \$67.1 billion takeover of Time Warner Cable Inc. and Bright House Networks LLC by Charter Communications Inc., as well as AT&T Inc.'s proposed \$48.5 billion purchase of DirecTV.

Because landlines are dying, VoIP providers must sell 24-hour batteries **from Ars Technica by Jon Brodtkin**

As phone providers like AT&T and Verizon seek to phase out copper telephone networks in favor of fiber- and wireless-based VoIP (Voice over

Internet Protocol) services, the Federal Communications Commission must consider whether to require home phones to work during power outages.

Mobile & Social

[SEC Looking Into Fake Web Report That Sent Twitter Up 8%](#) from Bloomberg News by Matthew Robinson and Jordan Robertson

The U.S. Securities and Exchange Commission is looking into possible market manipulation over a fake news article that led to a brief spike in Twitter Inc. shares, said a person familiar with the matter.

[Fake Twitter Story Fuels Worries with New Web Addresses](#) from National Journal by Brendan Sasso

A fake news article that caused Twitter stock to spike briefly Tuesday is underscoring concerns that a flood of new Web domains could empower fraudsters.

[Uber Could Have to Pay an Additional \\$209 Million to Reclassify Its Drivers in California](#) from Recode by Carmel DeAmicis

If Uber loses its lawsuit in California, it would have to pay roughly \$208.7 million a year. This breaks down to about \$89.1 million for payroll taxes for 45,000 drivers working 20 hours a week in the state, and roughly \$119.6 million per year in workers' compensation insurance. Altogether, it's \$4,637 per employee in California.

[Clinton's tech chief defends comments on Uber economy](#) from The Hill by Mario Trujillo

Hillary Clinton's campaign is firing back at the Republican field after comments she made about the so-called sharing economy drew criticism from some GOP presidential candidates.

Data

[ACLU to appellate court: Please halt NSA's resumed bulk data](#)

collection

from Ars Technica by Cyrus Farivar

The American Civil Liberties Union (ACLU) has asked one of the nation's top appellate courts to order the National Security Agency to stop its bulk records collection, which resumed in limited form last month as part of the USA Freedom Act.

Google accidentally reveals data on 'right to be forgotten' requests

from The Guardian by Sylvia Tippman and Julia Powles

Data shows 95% of Google privacy requests are from citizens out to protect personal and private information – not criminals, politicians and public figures

Advocating privacy

from The Hill by Cory Bennett

In just under a year, the think tank Georgetown Law's new Center on Privacy and Technology has become a respected voice in Washington, as Congress considers revamping privacy laws to match the ongoing revelations about government surveillance and the growing ubiquity of Internet-connected devices.

Amendment to create student data privacy commission clears

Senate

from FedScoop by Corinne Lestch

The panel would research which federal and state laws around student data privacy are working and which aren't.

Cybersecurity

U.S. has yet to notify 21.5 million data breach victims: officials

from Reuters by Mark Hosenball

Two months after discovering that sensitive personal information on 21.5 million Americans was compromised in a hack of government databanks, none of those affected has been officially notified.

Your Data Is Compromised. (Yes, Yours.) What Now?

from National Journal by Kaveh Waddell

The day after Nicolle Gallo's notification arrived in the mail, she spent half an hour signing up for the credit-monitoring and identity-fraud-protection service OPM offered her free of charge for 18 months, entering data like her passport number and health insurance information. And that was that. Gallo, now vice president of Ditto Public Affairs in New York City, has not since been contacted by OPM or CSID, the contractor providing the 18 months of services.

Federal cybersecurity incidents increased more than 1,000 percent since 2006

from FedScoop by Billy Mitchell

The two OPM hacks that compromised the personal information of 22.1 million people were just blips on the radar in total volume of federal cyber incidents.

How Much Damage Can the OPM Hackers Do With a Million Fingerprints?

from National Journal by Dustin Volz

The pilfering of 1.1 million fingerprints is "probably the biggest counterintelligence threat in my lifetime," one former NSA official said.

This 25-Year-Old Vietnamese Man Stole the Identities of Nearly 200 Million Americans

from Yahoo News by Alyssa Berezna

Vietnamese citizen Hieu Minh Ngo has been given a 13-year prison sentence for breaking into the computers of American companies, stealing personal information for nearly 200 million people, and selling it to other criminals online. The 25-year-old made more than \$2 million in the process.

FT Investigation: Cyber insecurity

from the Financial Times by Kate Scannell and Gina Chon

US agencies are responsible for vital interests lack basic IT defenses. An in-depth report.

Cyber insecurity: alert raised on aviation agency

from the Financial Times by Kate Scannell and Gina Chon

A government watchdog this year raised red flags over the agency in charge of US civilian flights and air traffic control systems for more than 19,000 airports, saying it has failed to implement a crucial security system.

IT budgets cut even as cyber threat grows

from the Financial Times by Kate Scannell and Gina Chon

IT spending at many of the US government agencies hit by devastating cyber attacks is being cut, even as the threat to national security and privacy is escalating, an analysis of budget reports has found.

Six Nigerians Extradited to US for Alleged Internet Scams

from Security Week by Agence France-Presse

Six Nigerian nationals have been extradited from South Africa for their alleged role in Internet scams involving dating websites and work-at-home schemes.

E-Commerce

Apple Pay launches in Britain as holdout Barclays signs up

from Reuters by Eric Auchard

Apple introduced its mobile payments service to Britain on Tuesday as Barclays became the last major UK bank to sign up for the U.S. tech giant's effort to capitalize on the increasing comfort among British consumers with making tap-and-go purchases.

Opinions, Editorials & Perspectives

Why the Politics of Disruption Offers No Quick Fix for the Republican Party

from Morning Consult by Nick Gourevitch and Sophia Yeres

Employees from major Silicon Valley tech companies overwhelmingly donated to Democrats in the last three decades, according to a Crowdpac

analysis. And on the ultimate metric—voters—Millennials have supported Democrats by an approximately two to one margin in the last two presidential elections.

Why and How Congress Should Outlaw Revenge Porn

from the Information Technology and Innovation Foundation by Daniel Castro and Alan McQuinn

While a number of states and private businesses have taken up the cause to reduce revenge porn, it is not enough. Congress should take action to address the nonconsensual distribution of sexually explicit images.

Fed's Faster Payments Security Priorities

from Bank Info Security by Tracy Kitten

Gordon Werkema, who is leading the Federal Reserve System's initiative to revamp the U.S. payments infrastructure, says security issues must be addressed as the move toward faster payments progresses.

Research Reports, Issue Briefs & Case Studies

In Regulation and Investment: A Note on Policy Evaluation under Uncertainty, With an Application to FCC Title II Regulation of the Internet

from the Georgetown Center for Business and Public Policy by Rob Shapiro and Kevin A. Hassett

This report finds that the majority of economic literature and the prevailing economic theory about the impact of regulation on private investment in capital-intensive industries clearly refute the FCC's theories that Title II will grow investment in the Internet.

SUBSCRIBE

*The Morning Consult
Morning Consult, P.O. Box 27068
Washington District of Columbia 20038
United States*

This email is intended for david.shive@gsa.gov.
[Update your preferences](#) or [Unsubscribe](#)

Subject: Morning Consult Tech: Public Housing Residents to Get Low-Cost or Free Internet Access; Data Breaches Spur Growth in Cybersecurity Startups
From: "Morning Consult" <tech@morningconsult.com>
Date: 7/16/2015 8:35 AM
To: David Shive <david.shive@gsa.gov>

by [Amir Nasr](#) (@ameerkatmanor)

Today's Washington Brief

- President Obama announced a new program that will provide low-cost or free internet access to public housing residents. ([New York Times](#))
- Federal law enforcement authorities helped break up a network of cybercriminals that used the forum Darkode to buy and sell malicious software, stolen credit card data and lifted passwords. ([CNET](#))
- As lawmakers on Capitol Hill push for rules that would allow the use of more commercial drones, many U.S. voters aren't keen on seeing more of the unmanned aerial vehicles, at least when it comes to delivering packages. ([Morning Consult](#))

Today's Business Brief

- Cybersecurity startups are seeing a boost in investment funding following an increase in well-publicized, massive data breaches. ([Wall Street Journal](#))
- For a fourth time, a U.S. judge rejected a case against Google Inc. from users alleging the search giant had violated privacy laws, saying the plaintiffs failed to prove any harm came from Google's actions. ([Bloomberg News](#))
- Uber has been handed a \$7.3 million fine for its failure to disclose the number of requests for accessible vehicles from the California Public Utilities Commission. The company said it will appeal the decision, and if it doesn't pay the fine within 30 days it will lose its operating license in California. ([Recode](#))

Today's Chart Review

[After Netflix Stock Split, Should I Buy NFLX?](#)
from Money Morning

Mark Your Calendars (All Times Eastern)

Thursday

Defense One holds an [event](#) called "Anticipating the Next DOD Insider Threat" @ 8:30 a.m.

The [Internet Governance Forum](#) will discuss various issues arising on the internet from government officials, private sector experts, Hill staff, academics and advocates @ 9 a.m.

The FCC [holds](#) an open meeting @ 10:30 a.m.

Politico hosts a [discussion](#) titled "Outside, In: Aging in a Tech World" @ 11:45 a.m.

Earnings Report: [Google Inc.](#)

Friday

Advisory Committee to the Congressional Internet Caucus holds a [briefing](#) titled "Taylor Swift or Congress? Who Has More Power in the Digital Music Streaming Marketplace?" @ 12 p.m.

TechFreedom hosts [event](#) on "restoring Internet independence," featuring remarks from FCC Commissioner Ajit Pai @ 8 p.m.

Earnings Report: [NetScout Systems Inc.](#)

General

[U.S. Program Will Connect Public Housing Residents to Web](#)
from the New York Times by Dionne Searcey and Peter Barker

The Obama administration announced a program to connect thousands of public housing residents across the nation to the internet at low prices or

free, part of a broader effort to close the so-called digital divide and help low-income Americans succeed in a technology-driven society.

Lawmakers Out of Step with Voters on Commercial Drones **from Morning Consult by Tess Danielson**

The House Committee on Small Business on Wednesday held a hearing to discuss the benefits of expanding the use of drones for commercial projects. But many of their constituents are less than enthused about seeing more small, remote-controlled aircraft, especially around their homes and offices.

Report pushes Congress to ban revenge porn **from The Hill by Lydia Wheeler**

A D.C.-based think tank is calling on Congress to ban revenge porn – pornography posted to the Internet without the consent of those depicted. The report recommends Congress pass legislation like the bill Rep. Jackie Speier (D-Calif.) is preparing to unveil on July 23, create a special unit in the FBI to provide immediate assistance to revenge porn victims and direct the Department of Justice to work with the private sector on developing best practices for how online services can quickly remove nonconsensual pornography.

How a Federal Employee with Fake Diplomas Worked at the Department of the Interior for Five Years **from National Journal by Kaveh Waddell**

A federal employee occupied a high-ranking technology position at the Interior Department for several years before an investigation found that he had faked his education.

Former majority leader lobbying for online gambling opponents **from The Hill by Mario Trujillo**

Former Senate Majority Leader Trent Lott (R-Miss.), former Sen. John Breaux (D-La.) and a host of other former congressional staffers will lobby for a group pushing a ban on Internet gambling. The Coalition to Stop Internet Gambling — backed by GOP donor and casino owner Sheldon Adelson — hired the lobbying firm Squire Patton Boggs.

European Stocks Rise as Greek Approval Clears Euro-Area Outlook **from Bloomberg News by Alan Soughley and Sofia Horta E Costa**

The Stoxx 600 added 1.3 percent to 405.4 at 12:46 p.m. in London. Optimism over a resolution of the Greek crisis has helped the Stoxx 600 rebound 8.8 percent from a July 7 low, after falling almost 10 percent from an April record. Federal Reserve Chair Janet Yellen on Wednesday delivered an upbeat message on the economic outlook and repeated that the Fed is likely to raise its main interest rate this year.

Immigration

How Better Tech Can Make the Immigration Process Suck Less **from Wired by Issie Lapowski**

Along with the Department of Homeland Security and Department of State, the White House enlisted the help of the new U.S. Digital Service team, led by former Google engineer Mikey Dickerson, to find a way to streamline the immigration process with technology.

Net Neutrality

How a bitter clash at the FCC is gumming up one of the most important issues in tech **from the Washington Post by Brian Fung**

Bowing to pressure from congressional Republicans, Tom Wheeler, the chairman of the Federal Communications Commission, won't be holding a hotly anticipated vote this month on rules for a looming, high-stakes auction of wireless airwaves.

Intellectual Property

House pushes back vote on patent reform **from The Hill by Mario Trujillo**

House Republicans are delaying a vote on patent reform legislation, House Majority Leader Kevin McCarthy (R-Calif.) told lawmakers, amid concerns about the bill. Judiciary Chairman Bob Goodlatte (R-Va.) said the

committee would use the extra time to try and grow support.

Telecommunications

[Netflix Lends Support to Charter-Time Warner Cable Deal](#) from the Wall Street Journal by Shalini Ramachandran

Charter Communications Inc. has won the support of a major player in its bid to win regulatory approval for the Time Warner Cable acquisition: Netflix Inc.

Mobile & Social

[Uber Fined \\$7.3 Million for Not Reporting California Accessibility Data](#) from Recode by Carmel DeAmicis

The California Public Utilities Commission (CPUC) slapped Uber with a \$7.3 million fine for failing to provide information on how many requests it receives for accessible vehicles. Uber has 30 days to pay the fine or lose its operating license in California. Uber said it will appeal the decision and there will be no suspension during the appeal process.

[Mexico City unveils first regulation on Uber in Latin America](#) from Reuters by Max de Haldevang

Mexico City became the first city in Latin America to regulate Uber, announcing rules that include a 1.5 percent ride levy, a yearly permit fee and a minimum vehicle value.

Data

[Google Wins Bid to Toss Suit Claiming Privacy Violations](#) from Bloomberg News by Joel Rosenblatt

Google Inc. users were blocked from suing over alleged privacy violations by a judge who said they failed to show any of their information had been disclosed. It was the fourth time U.S. Magistrate Judge Paul Grewal rejected the case.

[Can NOAA pay industry to fill its weather data gap?](#)

from FCW by Zach Noble

At a hearing of the House Science, Space and Technology Committee's Environment Subcommittee, Manson Brown, deputy administrator at the National Oceanic and Atmospheric Administration, discussed the promise of private-sector involvement and the treaty obligations that hold weather data to be a public good, distributed free of charge.

Cybersecurity

[Data Breaches Boost Funding for Cybersecurity Startups](#)

from the Wall Street Journal by Danny Yadron

"Security startups never really did so well," says Mr. Krohn, who studied computer science at Harvard University and the Massachusetts Institute of Technology. "There was not an example of a runaway success." That is changing, following major data breaches, as corporate customers and venture capitalists show increased interest in cybersecurity.

['Darkode' goes dark: Police shut down infamous cybercrime marketplace](#)

from CNET by Edward Moyer

The FBI and the US Department of Justice have helped break up a massive and notorious one-stop shop for cybercriminals, an online marketplace where hackers and others worldwide could buy and sell malicious software, stolen credit card data, lifted passwords and more.

[Draft IG audit finds thousands of cybersecurity vulnerabilities at Interior Department](#)

from FedScoop by Whitney Blair Wyckoff

About 3,000 critical and high-risk vulnerabilities were found in several of the Department of the Interior's bureaus, according to a yet-unreleased draft inspector general report discussed at a House oversight panel hearing.

[CSIS, lawmakers launch cyber task force for next president](#)

from FCW by Sean Lyngaas

The next president won't take office for another 18 months, but there is already a task force to advise him or her on the critical job of improving the nation's cybersecurity.

NSA Chief Expects More Cyberattacks Like OPM Hack
from the Wall Street Journal by Robert Wall and Alexis Flynn

The U.S. should brace itself for more attacks like one on the U.S. Office of Personnel Management—in which millions of sensitive government records were stolen, the director of the National Security Agency warned.

OPM Says 84,000 Hack Victims Still Not Notified
from NextGov by Aliya Sternstein

Nearly 40 days after the Office of Personnel Management divulged that attackers copied millions of government employee personnel records, the agency says it's alerted 98 percent of affected employees. That, however, still leaves 84,000 individuals who have not been notified their privacy has been compromised.

The OPM breach exposed more than a million fingerprints. Here's why that terrible news.
from the Washington Post by Andrea Peterson

The scariest part of the massive hack at the Office of Personnel Management may not be the breach of Social Security numbers or employment information. Instead, it could be something closer to home — in fact, just on the tip of your fingers: The breach exposed more than 1 million fingerprints to hackers. And unlike an address or even a Social Security number, those fingerprints can't be changed.

An Identity Thief Explains the Art of Emptying Your Bank Account
from Bloomberg News by Dune Lawrence

Nightfall in Minsk means Dmitry Naskovets begins working the phone. At 24, Naskovets is tall and skinny, and still looks like the college kid he recently was. He's in his apartment's kitchen, in a respectable neighborhood off the second ring road in the capital of Belarus. He starts around 6 p.m. and usually doesn't quit until three the next morning.

E-Commerce

EBay Nears Deal to Sell eBay Enterprise Unit for Around \$900 Million

from the Wall Street Journal by Greg Bensinger and Gillian Tan

EBay Inc. is closing in on a deal to sell its eBay Enterprise unit to a group led by private-equity firm Permira for around \$900 million.

Opinions, Editorials & Perspectives

Hacked? Big deal: I made my most personal data public

from Politico by John Halamka

A Harvard doctor and tech expert explains why he posted his own health records on the Web — and why society should make a radical leap.

Do Encrypted Phones Threaten National Security?

from The Atlantic by Conor Friedersdorf

In Washington, D.C., where a growing chorus is demonizing end-to-end encryption that permits people to have conversations that the government can never see, Senator Sheldon Whitehouse has aired a particularly extreme anti-privacy position: The Rhode Island Democrat suggested last week that selling well-encrypted smartphones to Americans should be treated like dumping toxic waste in streams.

Tech policy belongs on the 2016 campaign agenda

from Computer World by Richard Adler

The next race for the White House is already well under way, with candidates in each party formally announcing their intention to run for the presidency on a regular basis. One topic that seems unlikely to get much traction is telecommunications and technology and the policies that regulate them.

Why privacy alarmists are wrong about data rules in big trade deals

from the Christian Science Monitor by Stephen Ezell

Provisions in the Trade in Services Agreement, which is currently under negotiation in Geneva, are not meant to erode privacy. Instead, the pact reflects the reality of how data is stored and transmitted in the modern global digital economy.

Research Reports, Issue Briefs & Case Studies

The Evolving Role of News on Twitter and Facebook from Pew Research Center by Michael Barthel et al.

The share of Americans for whom Twitter and Facebook serve as a source of news is continuing to rise. This rise comes primarily from more current users encountering news there rather than large increases in the user base overall.

SUBSCRIBE

*The Morning Consult
Morning Consult, P.O. Box 27068
Washington District of Columbia 20038
United States*

This email is intended for david.shive@gsa.gov.
[Update your preferences](#) or [Unsubscribe](#)

Subject: Morning Consult Tech: Silicon Valley Donating More to Presidential Candidates; Android Users' Lawsuit Against Google Dismissed
From: "Morning Consult" <tech@morningconsult.com>
Date: 7/17/2015 8:51 AM
To: David Shive <david.shive@gsa.gov>

by [Amir Nasr](#) (@ameerkatmanor)

Today's Washington Brief

- Visits from politicians to Silicon Valley to secure donations for campaigns have increased since 2008, with the most recent one by Republican presidential candidate Jeb Bush. ([Venture Beat](#))
- Uber has not only shaken up the U.S. taxi industry, it's also now a central topic of debate for Democratic and Republican presidential candidates. ([New York Times](#))
- The Office of Personnel Management faces a tough prospect in providing credit monitoring for more than 20 million people affected by a recent data breach. ([Morning Consult](#))

Today's Business Brief

- A judge dismissed a lawsuit filed by Android users against Google Inc. that said the company had violated its own privacy policy by disclosing customer names, email addresses and account locations to third parties without the users' permission. ([Reuters](#))
- eBay is set to complete its PayPal spinoff, a move that could prove challenging for the e-commerce giant as it jettisons assets amidst shrinking sales. ([Wall Street Journal](#))
- Google's stock rose after it reported increased revenue of 11 percent to \$17.7 billion. Search traffic, mobile usage and YouTube viewership were all hailed as crucial to the gains. ([Washington Post](#))

25 February 2010

PCO's Final Offer – Alternate B to immixTechnology

Attachment A

MANUFACTURER TO BE DELETED
3PAR GOVT SYSTEMS
ACCESSDATA
ALTOBRIDGE
ANAKAM
ANTS SOFTWARE
APPLIMATION
APPROVA
ARCHIBUS
ARCSIGHT
ARIBA
ART TECHNOLOGY GROUP (ATG)
ATOMICA
ATTACHMATE
AXYN TECHNOLOGIES
BANTU
BIVIO NETWORKS
BLUEARC
BLUECAT NETWORKS
BRASSRING TECHNOLOGIES
CA / NETEGRITY
CABLE & WIRELESS
CADENZA, INC.
CARRIER ACCESS
CARTESIS, INC.
CLOAKWARE
COMPOSITE SOFTWARE
CORETRACE
COUNTERPANE INTERNET SECURITY
DAON
DATABEACON
DATARAM
DECISION LENS
EGENERA
EIGNETWORKS

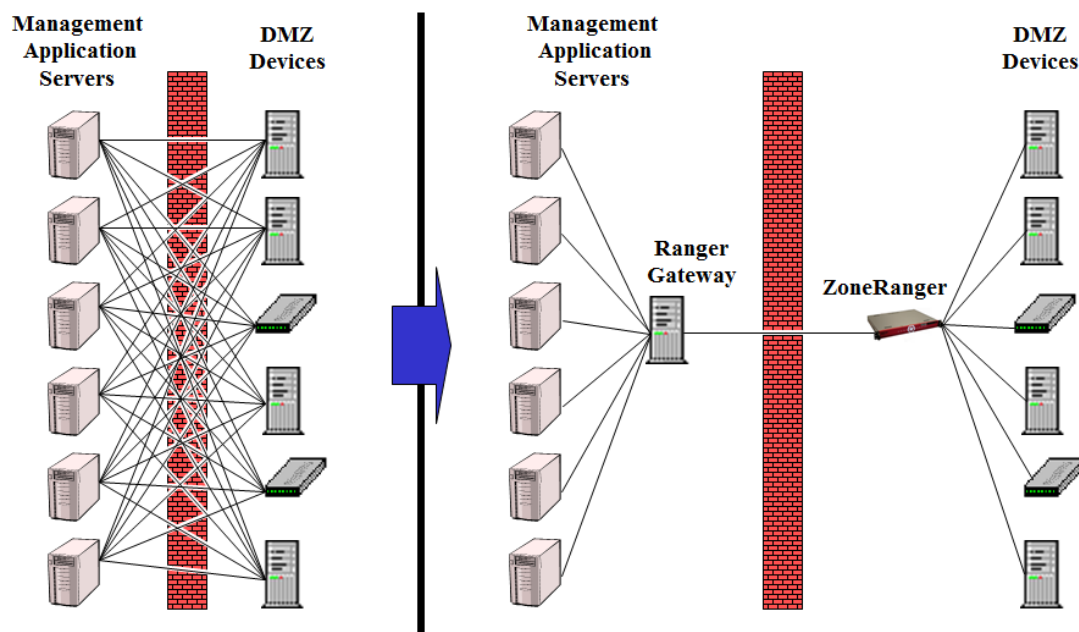


CAPABILITIES AND IMPACT ASSESSMENT

Tavve is a US-based and US-owned private software company. Tavve is currently managed under the PISA program. The first KMP was issued clearance in December 2014. Tavve's market focus and subject matter expertise is network management, operations, and security. Tavve's base product platform is the ZoneRanger. The ZoneRanger was designed and built as a highly secure, network-hardened appliance. The initial release provided an SNMP proxy capability for HP Network Node Manager (NNM). The current release supports proxy for SNMP, SNMPv3, ICMP, Telnet/SSH, FTP, SCP, SFTP, TFTP, NTP, TACACS+, Radius, HTTP, and HTTPS. Inbound UDP traffic flows include Syslog, Netflow, and SNMP Traps. For all of these protocols, the ZoneRanger, Firewall(s), and RangerGateway are 100% transparent to the management application and downstream devices. The ZoneRanger has three deployment models:

- 2U redundant, rack-mounted appliance
- Virtual Appliance (VMware)
- Cisco UCS Express or UCS E-series embedded application

The ZoneRanger's value proposition impacts two areas. First is the elimination of open firewall ports and the underlying firewall rules for all management protocols. With the exception of HTTPS and SNMPv3, all of the industry standard protocols are unencrypted and easy to spoof. The ZoneRanger performs a deep packet inspection of each of these protocols, rebuilds the packets, and encrypts the transmission, while removing all forensic data (ip addresses, hostnames, community strings, etc) from the initial message. The elimination of open management protocol ports dramatically reduces the firewall attack surface.



The second area impacted by the ZoneRanger is change control. By eliminating the requirement for open management ports, there are no requirements for the hundreds to thousands of firewall rules to open and manage those ports. This single feature gives the ZoneRanger an ROI of less than six months in most cases. Without the burden of firewall rules, firewall committees, and the required documentation,

deployment speed is increased, labor requirements are dramatically reduced, and eliminating the human error of writing firewalls rules further increases overall operational security. In most cases DMZ access is an unhappy compromise between network operations and security. Network operations needs to reach every device while the security team grants DMZ access on an exception basis. The end result is neither party is happy or able to fully address their job requirements. The ZoneRangers dramatically reduces the attack surface while giving the operational team full access to all downstream devices with encrypted and authenticated messages.

Initial ZoneRanger deployments were exclusively focused on perimeter devices (border, DMZ, edge). Over time the ZoneRanger's role has expanded to core networks for ACL concentration and network management data caching. When deployed as a core network UDP receiver, the ZoneRanger can be utilized to consume, filter, and re-distribute Syslog and/or Netflow to an unlimited set of destinations.

The ZoneRanger is vendor independent. This includes management applications, firewalls, and end-devices. The ZoneRanger is deployed by 21 customers in 13 countries. These installations fall into three primary market sectors:

- financial institutions
- managed service providers (MSPs)
- government

One of these customers is a FVEY partner (UK). This customer initiated our PISA request and NSA sponsorship. A major requirement for this customer/project was a CESG audit and certification.

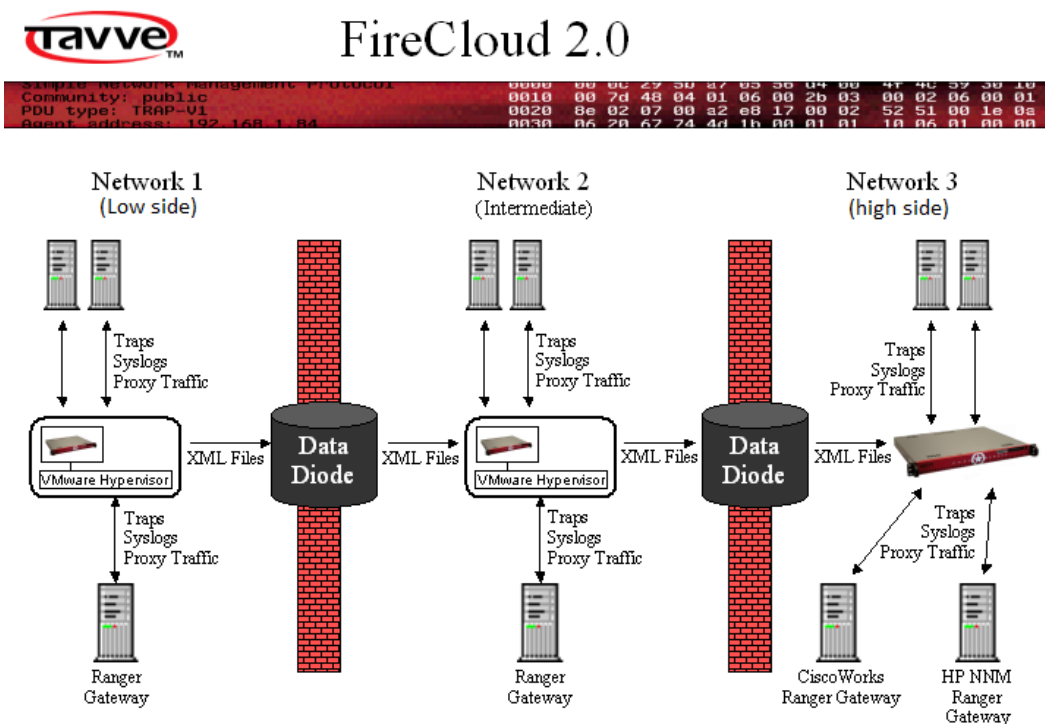
Across this broad customer base, the following management applications are deployed in conjunction with the ZoneRanger:

- CA UniCenter
- Cisco ACS (TACACS+)
- CiscoPrime (CiscoWorks)
- eHealth
- EMC Smarts (Ionix)
- Entuity (Eye Of The Storm)
- HP NNMI
- HP Operations Manager (OM)
- HP SiteScope
- HPNA
- IBM NetCool
- In-house custom applications based on supported protocols
- Infovista
- NetQOS
- NetScout
- OpenNMS
- PRTG
- Radius Authentication
- SIEMs

- Solarwinds
- Splunk

In addition to the industry standard protocols and standard networks, there are four add-on products. These products expand the functionality to address specific technical requirements and/or environments. These four products are:

- HP Operations Manager – This add-on feature allows HPOM agents in the DMZ to communicate with the management console. Requests can be initiated from the agent (DMZ) or console (CORE).
- VOIP Handset – Specific features to allow verification of a VOIP handset against certain stored information prior to permitting boot requests to the VOIP call manager.
- Inbound TCP Proxy – With the exception of TACACS+ and Radius requests, the ZoneRanger automatically denies unsolicited inbound TCP requests. This feature allows TCP requests to be initiated from the DMZ.
- FireCloud – The unique solution was built in partnership with our FVEY customer. The requirement was to keep their air-gapped networks intact, but allow almost real-time monitoring of low-side networks. Using a complex and highly secure XML transport model, low-side ZoneRangers and their respective networks push customer selected management upstream via a series of data diodes and other classified components.



Please see tavve.com for additional information. No cost evaluation units or virtual appliances are available for testing. Direct inquiries should be sent to Doug Austin. He can be reached at doug.austin@tavve.com or 919-235-8476 (non-secure).

Technologist, Technology Consultant, and Advisor

Education

MBA with emphasis in Technology Management from the University of Phoenix
BS in Business from Regents College
32 Semester hours towards PhD in Information Technology
Multiple post graduate courses in information technology and information security

Training

CISSP (exp), CEH (exp), ISA (exp), Security + (exp)
Former government ISSM and FSO, DoD Level I, II, III System administrator (exp), Government Red Team member, penetration tester, information technology policy technical writer. Information technology policy, contract technical writer, for the banking, insurance and healthcare industries.
Currently working to complete the CSA (Certified Security Auditor) certification.

ISO Certifications as a lead auditor for:
ISO 9001: 2015 - Quality Management Systems
ISO 20000-1:2011 - IT Service Management
ISO 22301:2012 - Business Continuity Management
ISO 27001:2013 - Information Security Management

ISO Implementer training and experience for:
ISO 9001: 2015 - Quality Management Systems
ISO 20000-1:2011 - IT Service Management
ISO 22301:2012 - Business Continuity Management
ISO 27001:2013 - Information Security Management
ISO 28001:2007 - Supply Chain Security
ISO 31001:2009 - Risk Management
ISO 9075-1:2011 - Information Technology – Database

Auditing, policy writing, and system implementation experience with US government laws, regulations, and policies including:
(GLBA) Gramm–Leach–Bliley Act, (FISMA) Federal Information Security Management Act, (HIPAA) Health Insurance Portability and Accountability Act, (FIPS) Federal Information Processing Standards, Homeland Security Act, (NIST) National Institute of Standards and Technology - Cybersecurity Framework, (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations, (NIST) Special Publication 800-150 (Draft) Guide to Cyber Threat Information Sharing, National Strategy for Global Supply Chain Security, (NSDD 145) National Security Decision Directive 145, (NSPD 38) National Security Presidential Directive 38, (NSPD 54) National Security Presidential Directive 54, (PPD 20) Presidential Policy Directive 20, (US-CERT) U.S. Computer Emergency Readiness Team – Security publications series, (NSA) National Security Agency - Security Configuration Guides

OEM Manufacturer pre-sales engineer level training with VAR certification on security related products from:

Bit9, Blacksquare, Bluecoat, CA, Checkpoint, Cisco, DB Networks, FireEye, F-Secure, Infoblox, MacAfee, Netscout, Palo Alto, Radware, RSA, Solarwinds, Sophos, Splunk, Strikeforce, Symantec, Trend Micro, Tripwire, Unisys, Watchguard, Websense

OEM Manufacturer pre-sales engineer level training with VAR certification on hardware solutions, including security, from:

Brocade, Cisco, Dell, EMC, F5, Hitachi, HP, IBM, Juniper, Netapp

OEM Manufacturer pre-sales engineer level training with VAR certification on software solutions, including security, from:

Adobe, Citrix, ESRI, Microsoft, Oracle, Red Hat, Sage, Salesforce.com, SAP, VMWare

OEM Manufacturer presales engineer training from over 1000 companies including more than 100 security companies or technologies

Implementation training and customer experience for:

CMMI - Capability Maturity Model Integration,

ITIL - Information Technology Infrastructure Library for IT Service Management (ITSM)

Risk Assessment - Validation of risk policy and practice using a structured methodology

Risk dash boarding - Visual representation of real time risk status against assessment

Security Assessment - Validation of security policy and practice using a structured methodology

Security dash boarding - Visual representation of real time security status against assessment

Supply Chain Security - Enhance the end-to-end integrity of the supply chain

Project Management – PMP (exp), Doctoral courses in project management, multiple enterprise level government and commercial projects as program manager or project management lead

Software development – Multiple government and commercial enterprise software projects with direct and multi-level reports

Quality – Skill examiner and lead implementer in multiple ISO disciplines, ITIL v3 Foundation, Training in Agile, SCRUM, LEAN, and Six Sigma software design and testing methodology

Change management – Multiple government and commercial enterprise software lifecycle projects

Networking – BCNA, BCFA, CCNA (exp), CNE (exp), MCSE (exp), Network + (exp), A+ (exp) managed network and web based projects in multiple Defense megacenters

Cloud Methodology – Multiple cloud deployments in FEDRAMP Datacenters, Defense megacenters, and commercial tier 1 datacenters.

Datacenter – Designed systems in over ten different government datacenters, as well as design and consulting in dozens of commercial datacenters

Server/storage – 20 years of server/storage training and experience

Virtualization – VCP, CCA (exp), former VMWare advisory board member

COTS – 20 years of government and commercial software evaluation and deployment experience

Physical Security – Training and implementation experience with perimeter and building access control systems, camera systems, (PSIM) Physical security information management systems, automation and control systems, alarm systems, sensor systems, dispatch and monitoring centers, emergency operation centers, SCIF design course, datacenter design and protection, disaster recovery/continuity of operations, facility management, executive protection, tactical threat assessment, tactical response, former NREMT-P, Former Firefighter I,II,III

Open source – Designed and operated websites with 7 different types of open source software. Frequent contributor to the open source software institute

E-commerce – Designed and operated four different commercial e-commerce websites

Social media – Post graduate training on advanced social media utilization, marketing, and statistical analysis

Acquisition Planning – Former government contract officer, Certified Acquisition Strategist.

Experience

Opsis Group

As the CEO and principal consultant of the Opsis Group of companies, I have the ability to further my efforts as a practicing technologist in the information technology industry. I research and interact with cutting edge technology companies on a daily basis. I use my extensive connections (3000+) with national Value added resellers (VAR) and system integrators (SI) to bring this technology to market in the government and commercial sector. I continuously work on significant issues with customers and provide unique and innovative solutions using technology solutions.

Affigent

I was the Chief Technologist and Director of Engineering for Affigent LLC, a reseller of technology services and solutions to the U.S. Federal Government. In this role I recruited, trained, and led a team of pre-sales engineers trained to identify and solve customer technology issues. I acted as a technology evangelist speaking at conferences, authoring articles, and participating in media interviews. I created the security practice, with an emphasis on 360 degree security protection that includes cyber security and physical security in one protection envelope, and trained the security team on technologies, practices, and policy. I conducted extensive customer engagements evaluating identified and discovered issues, and providing solutions to manage security risks.

Brocade

I was the Channel engineering manager responsible for supporting the U.S. Government channel. I led the field engineers in supporting all of the government VAR's sales and support efforts on a global basis. I was a member of the corporate software design and review team. I

worked with the Worldwide Vice President of System Engineering to develop policies, plans, and professional development training for the global system engineering workforce.

CDW

I was the Chief Technologist for CDW. I began at CDW as the Chief Technologist for CDW Government and managed the government pre-sales engineers. CDW then merged the pre-sales engineering roles for government and corporate into one team that I managed. This also changed my role to the Chief Technologist for all commercial and government groups within CDW including CDW Canada. I managed all vendor evaluations, sat on the new vendor add committee, managed all customer demo labs, and managed all shows and events technical solutions and support. I authored the CDW technical training curriculum for engineers, and the sales technical quickstart program. I managed the design implementation of the CDW sales technical configuration cloud portal. I spoke at conferences and shows, authored papers, and participated in media interviews. I sat on the advisory board for multiple technology companies. I was the enterprise level architect for fortune X customers and high priority projects, and interacted with C level corporate officers, General officers, SES level government officials, as well as owners and executive staff at technology solution companies. I evaluated customer environments, proposed technology solutions, and managed the implementation of complex hardware, software, and services capabilities to fill customer needs.

GTSI

I was the Lead Technologist and Strategic Account Team Manager for GTSI (Now Unicom Government). I conducted vendor evaluations and sat on the new vendor add committee. I was an enterprise level engineer for government customers and high priority projects. I evaluated customer environments, proposed technology solutions, and managed the implementation of complex hardware, software, and services capabilities to fill customer needs. I was a foundation member of the security evaluation team that provided evaluation, training, and professional services in security to government agencies.

DISA

I held a multiple employee sub-contract, and filled a contractor position at the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) Defense Megacenters (DMC) Ogden. I was a principal architect, program manager, project manager, and business development lead. I sat on the DISA Computing Services engineering review board that designed enterprise solutions and controlled technology acquisition. I program managed multiple government programs. I designed several technology solutions for government programs. I authored the site security policy and standard operating procedures for the non-mainframe groups. I worked with multiple DOD agencies to design and source systems to manage and protect their data. I achieved the highest level of system administrator training and certification in operations and security. I attended classified and unclassified training for DOD and government security policy, procedures, and technology.

Other

Active DoD Top Secret Security Clearance

TSA Security Clearance in progress

Military Veteran - US Army, US Army Reserve, Utah National Guard